CYBERARK

SOLUTION BRIEF

GDPR PRIMER FOR THE C-SUITE AND BOARD OF DIRECTORS

The intent of the EU Council's General Data Protection Regulation (GDPR) is to better address the protection of personal data. Here's a quick look at what executives and board members need to know.

Fast Facts

What is GDPR	The EU Council's General Data Protection Regulation replaces and greatly expands upon Data Protection Directive 95/46/EC.
Who is affected by GDPR?	Any business that collects or processes the personal information of EU citizens and residents – regardless of business location.
What is the financial impact of GDPR?	Noncompliance can result in fines of up to 4% of annual global turnover, or 20million Euro (whichever greater of the two). Individuals have the right to receive compensation from the controller or processor for the damage suffered as a result of such noncompliance.
Who enforces GDPR?	Each EU Member State appoints one or more Supervisory Authorities to implement and enforce GDPR.

Avoiding Penalties

Demonstrating that reasonable controls for protecting personal data have been put in place may aid an organization in avoiding penalties and liability from individuals' rights to compensation. Importantly, you should control who has access to that data.

- **Know your personal data.** Assess the risk to the personal data you hold and use: clearly identify what personal data you collect, where and how you store and use personal data.
- **Know who has access.** You should know who has access to personal data, including access by third party processors and vendors.
- **New GDPR requirements.** Controllers should have in place mechanisms for data subject consent, the right to erasure, the "right to be forgotten", the right to data portability, training staff, audits and privacy impact assessments, implementing privacy "by design", and more.
- **72 hour notification.** A controller must generally notify the Supervisory Authority (SA) of any personal data breach within 72 hours of discovery. This includes an accounting of what records, how many likely impacted, and steps taken to mitigate the breach.
- **DPO.** For many businesses, you must appoint a Data Protection Officer (DPO)

GDPR Presents Opportunities	
Today	**Looking forward**
Responsible custodianship of personal data protects your revenue stream—customer loyalty, customer retention, gaining new customers, and increasing their lifetime value.	The ability to demonstrate compliance not only strengthens your customer relationships, but can enhance brand, attracting new customers, new employees, better partners, and more business.
GDPR regulates third party vendors that process personal data. Compliant third party relationships keeps your partnerships strong and running smoothly.	A proactive approach to protecting personal data gives you the freedom to securely leverage business intelligence and can aid, even drive, the digital transformation of your business.
Securing personal data by design leads to a better security posture for other valuable corporate data such as trade secrets, financial information, contracts and legal documents, etc.	Compliance done right (i.e., up front, by design) carries forward into new processes and applications easily as new requirements emerge.

The Role of Privileged Account Security

GDPR compliance would be very difficult without a strong privileged account security strategy. Securing the privileged pathway to the systems containing personal data enables a business to proactively lock down access to sensitive systems and applications, enabling better control over who and what have access to personal data. Better access control helps you to tightly control your pathways to privileged access so unauthorized users and access are blocked.

For additional resources, visit www.cyberark.com/GDPR